

~~S-E-C-R-E-T~~

IBSEC-CSS-M-22

23 March 1970

COMPUTER SECURITY SUBCOMMITTEE
OF THE
UNITED STATES INTELLIGENCE BOARD
SECURITY COMMITTEE

Minutes of Meeting
Held at CIA Headquarters
Langley, Virginia
23 March 1970

1. The Twenty-Second meeting of the Computer Security Subcommittee of the United States Intelligence Board Security Committee was held on 23 March 1970 between 0930 and 1215 hours in Room 4E-64, CIA Headquarters Building. In attendance were:

[Redacted]

STAT

Mr. Richard F. Kitterman, State Member

[Redacted]

STAT

Mr. Thomas A. Eccleston, Army Member

Mr. Robert B. Cameron, Navy Member

Lt. Col. Charles V. Burns, Air Force Member

[Redacted]

STAT

Mr. Donald R. Roderick, FBI Member

[Redacted]

STAT

Mr. Carl R. Lambert, Navy

Mr. William S. Donaldson, Air Force

Mr. John Skaggs, FBI

[Redacted]

STAT

~~S-E-C-R-E-T~~

2. The security level of the meeting was announced as Top Secret COMINT.

3. Approval of Minutes: Omission of the word "Committee" was noted on page 4, paragraph 11 of the minutes of the 9 March 1970 Computer Security Subcommittee meeting. The Chairman requested that the individual Committee members correct their copies of the minutes. The Chairman also asked that the record copy of the minutes be appropriately corrected.

4. Training Course Task Report -- Discussion: The Chairman asked that the individual CSS members state their comments regarding the proposed agenda for the Computer Security Training Course which was distributed by the task team chairman during the 9 March 1970 meeting.

5. The CIA member began the discussion by indicating that he had coordinated the proposed agenda with Office of Computer Services experts and Office of Security Training personnel. Comments indicated the belief that the agenda for the afternoon of the third day could be expanded to include more detail as to what type hardware protect features should be covered. This section should at least include some explanation of all hardware components which have security aspects relating to them. On the fourth day more time should be allotted to the topic of emanations. In this respect [redacted] advised that the CIA Communications Security Office would be willing to provide Subcommittee members with a briefing regarding the specific problems of emanations as they relate to the computer environment. All members agreed that such a briefing could be of value and the CIA member indicated that he would make the appropriate arrangements.

STAT

6. Further suggestions from the CIA member noted that on the morning of the fifth day the topics of red/black installation criteria and emanations should be included as part of the inspection/certification process. From the seventh to the ninth day it was suggested that Technical Security considerations, as they relate to the problem of emanations, should be an integral part of the security survey process.

S-E-C-R-E-T

7. The Communications Security Office of CIA indicated their willingness to assist in any technical survey briefings conducted during the computer security training course. In addition, this office indicated a desire for certain members of their staff to attend the training course. They also suggested that certain selected personnel employed in the computer complex should also be eligible to attend the proposed computer security course.

8. The Army member recommended that during the afternoon of the first day an additional section be added under the title of "System Security (Equipment Measures, Software, etc.)."

9. During the afternoon of the second day it was suggested that examples of several network operations be discussed. In addition to the COINS network, it was recommended that discussion be held concerning other systems such as ANSRS, and CIA Time-Sharing.

25X1

10. During the morning of the third day a section F should be included under the title of "Software Penetration". The morning of the fourth day should include an additional section covering the topic of the laser burned belt. Mr. Lambert, U. S. Navy Technical Advisor, suggested that this section should also consider computer output microfilm and various aspects of micro-film storage.

11. The Army member concluded by stating that Army training personnel believed the course could be reduced to eliminate possible duplication with the current DODCI course. The Chairman indicated a belief that the computer security course could not be reduced any further and noted that the Computer Security Subcommittee thoroughly discussed the possibility of duplication with the DODCI course with the conclusion that the DODCI curriculum was not sufficient to satisfy the requirements of the Intelligence Community.

12. The NSA member felt that the entire curriculum should be built upon stated objectives. An attempt should be made to characterize the type of systems upon which computer security is built. During the first day, examples should be given as to how

S-E-C-R-E-T

S-E-C-R-E-T

the conclusion was developed that a security threat actually exists in a computer environment. Following this the course should then launch into the known and postulated threats of the computer complex and outline all the computer security considerations. These would include all the classical access schemes in the areas of personnel, physical, software, hardware, crypto and penetration attempts.

13. During the second day methods of application of systems should be discussed. This discussion should begin with simple systems and those security considerations which are relevant in such systems. This topic can then be expanded to include security problems inherent in more complex systems. The NSA representative questioned the outline on the morning of the third day in relation to the real difficulties of the various types of software programs which would be discussed. In addition, he suggested that the afternoon of the third day consider discussion regarding all types of hardware relating to a computer system. This should include such items as ancillary equipment, communication interface and various terminal disconnects.

14. The NSA representative felt that the topics to be covered on the fourth day were too extensive and should be split in half. The sixth day should then be used as a recap of the previous five day's training.

15. The NSA representative also stated the belief that the end of the fourth day would be a good point to break the two week instruction. The first four days would contain basic facts and principles relating to computer technology. The final six days will relate to actual use of these principles in developing a meaningful computer security program. In this respect, the NSA representative indicated that the final four days of the course are believed to be extremely valuable in that they offer actual contact with a computer system.

16. Finally in regard to the inspection/certification course indicated for the afternoon of the fifth day, NSA was of the opinion that it should be limited only to methods of inspection; the inspection aspect should prove sufficiently difficult without even attempting to discuss such an ill defined item as certification of the computer system.

S-E-C-R-E-T

S-E-C-R-E-T

17. The FBI member indicated that his agency would prefer to have more communication aspects considered during the course. The FBI representative believed that part of the sixth day should be altered to include a greater number of communication considerations.

18. Following this discussion the Chairman asked that each Subcommittee member submit his substantive comments in writing to the Training Course Task Team. He then asked that the Task Team expand upon their original outline by breaking down the subject matter into specific subject titles and allotting blocks of time to each title. This subject breakdown should also include a brief description of what each class will cover. Following this refinement the Chairman was of the opinion that consideration should then be given to developing a syllabus for the actual lectures.

19. Security Labeling Standards: The Chairman again requested submissions from those agencies who have not yet provided information regarding the security labeling standards within their individual organizations. He emphasized that completion of this initial collection effort is absolutely necessary before any other steps in this project can be undertaken.

20. Multilevel Operations: The Chairman apologized to Subcommittee members for not completing the promised draft papers on the subject of security requirements for multilevel operations and system security, test and evaluation. However, he noted that the delay was caused by the fact that he was not sure as to whether these papers should take the form of a DCID, a USIB guidance paper or a memorandum for members. At the instant meeting the Chairman asked that Subcommittee members provide any suggestions concerning this problem. The discussion indicated that these papers should consider only very broad and general requirements which would be acceptable to all members of the Intelligence Community. To do this the paper should be limited in scope to:

-5-

S-E-C-R-E-T

- a. Classified material within the Intelligence Community;
- b. Intelligence information outside the Intelligence Community;
- c. The three principal compartmented systems -- SI, TK, and B

All problems outside of the above areas would be addressed separately by the individual agencies. By limiting the scope of the papers to the above areas, it is hoped that the papers will be considered as policy guiding in nature.

21. Following the discussion the Chairman concluded that he is leaning toward the approach of having the papers take the form of a memorandum for the members. The memorandum would reflect broad policy guidance with actual implementation left up to the individual members.

22. System Security Analysis, Test and Evaluation:
The Chairman advised that the IHC recently ~~held~~ ^{at} another meeting ^{discussed} regarding the DIA ANSRS proposal ^{further}. ~~As a result of this meeting~~ a draft memorandum was drawn up in reply to DIA. The Chairman read the contents of the revised draft memorandum to the Subcommittee members and noted that the final draft will be sent to the DCI for his signature. Basically this memorandum is an IHC paper and has been coordinated throughout the IHC structure. In addition the Chairman of the IHC has also asked that the Chairman, Security Committee, sign the paper as a co-author. This paper has not yet been coordinated with the Security Committee. In this respect also recommended coordination of this paper with the Chairmen of the SIGINT and the COMIREX Committees. STAT

23. In reference to the proposed Subcommittee paper on guidelines for analyzing, testing and evaluating the security of community systems, the Chairman emphasized that any such paper would be an answer to the JCS and DSB papers which were previously written on this subject. The proposed CSS paper is intended to be a direct application of one of the conclusions of the DSB report and in no way is intended to be a duplication of effort.

S-E-C-R-E-T

24. The Chairman acknowledged that both of the above mentioned papers contained excellent points and wondered if it would be appropriate to quote some of the conclusions contained in these papers. It was concluded that this question would be answered when a final format had been decided upon. The Chairman stated that he will shortly complete a first draft of this paper for appropriate comments by Subcommittee members.

25. Other Business:

- a. The Chairman advised that as of 30 March 1970 he will attend a five-day seminar sponsored by the IBM Corporation at their Poughkeepsie, New York Office. This seminar is specially designed for members of the Intelligence Community;
- b. The Chairman indicated that he has received the final draft of the DSB report on security controls for computer systems. He noted that approval has been granted for public dissemination of this report; however, CIA has taken a position against any such dissemination. The CIA position against this dissemination is based upon the following reasons:
 - (1) The report would provide the opposition with substantial information as to which areas within the computer operations of the Intelligence Community are particularly vulnerable to penetration;
 - (2) Both NSA and CIA provided a wealth of information concerning the description of compartmented systems. Although this information was presented in a semi-sterile form, certain parts were included in the DSB report.

The Chairman indicated that CIA has requested a stay of publication until such time that they can present their views in writing.

-7-

S-E-C-R-E-T

S-E-C-R-E-T

26. The next meeting ^{is} ~~was~~ scheduled for 0930 hours
on 10 April 1970.



STAT

Executive Secretary
Computer Security Subcommittee

S-E-C-R-E-T

S-E-C-R-E-T

- a. Classified material within the Intelligence Community;
- b. Intelligence information outside the Intelligence Community;
- c. The three principal compartmented systems -- SI, TK, and B

All problems outside of the above areas would be addressed separately by the individual agencies. By limiting the scope of the papers to the above areas, it is hoped that the papers will be considered as policy guiding in nature.

21. Following the discussion the Chairman concluded that he is leaning toward the approach of having the papers take the form of a memorandum for the members. The memorandum would reflect broad policy guidance with actual implementation left up to the individual members.

22. System Security Analysis, Test and Evaluation:

The Chairman mentioned that the IHC had had further discussion at a recent meeting of the DIA proposal for Community sponsorship of a security test of ANSRS. At the request of the Chairman, IHC a memorandum had been drafted for the Chairman, USIB outlining the action recommended with reference to the DIA request. Preliminary coordination of this memorandum had been completed by the IHC and discussions with the Chairman, IBSEC and the Chairman, of the Computer Security Subcommittee had resulted in a redrafting of the memorandum. During the instant meeting the Chairman read the contents of the revised draft for member information. The paper is being prepared for the joint signatures of the Chairmen, IHC and IBSEC; it has not yet been coordinated with the Security Committee.

23. Concerning the proposed Subcommittee paper setting forth guidelines for analyzing, testing and evaluating the security of Community systems, a question was raised whether such a paper might be duplicative of the efforts of the Defense Science Board Task Team and the JCCRG Study Group. The Chairman noted

S-E-C-R-E-T

S-E-C-R-E-T

that the proposed Subcommittee paper would be an implementing document, where the DSB and JCCRG efforts were studies of the problem. No duplication is intended or foreseen. A second question was raised whether it would be useful to reference or quote from the DSB or JCCRG reports. The Chairman acknowledged that both of these papers contained noteworthy points; however, depending on the format of the Subcommittee papers on multi-level security and system security testing it may not be appropriate to reference or quote these other efforts. This question will be addressed when the final formats of the Subcommittee papers are decided.

24. Other Business:

a. The Chairman announced that he was attending a five-day executive seminar during the week of 29 March at the IBM Education Center in Poughkeepsie, New York. This seminar is offered to members of the Intelligence Community and is oriented to the latter's use of data processing techniques;

b. The Chairman also announced that he had received a copy of the final draft report of the Defense Science Board Computer Security Task Force. He indicated that its publication and dissemination is being delayed at the request of CIA to permit that Agency to examine the report's contents with a view toward making recommendations concerning the document's security classification. This examination is predicated on the OSD desire to approve the report for open publication.

25. The next meeting is scheduled for 0930 hours on 10 April 1970.

STAT



/ Executive Secretary
Computer Security Subcommittee

S-E-C-R-E-T